I CLAIM:

1. A computer program product operable to detect malicious computer program activity, comprising:

logging code operable to log a stream of external program calls;

primary set identifying code operable to identify, within said stream of external program calls, a primary set of one or more external program calls matching one or more rules indicative of malicious computer program activity from among a set of rules;

secondary set identifying code operable to identify, within said stream, at least one secondary set of one or more external program calls associated with said primary set of one or more external program calls; and

modifying code operable to modify said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity.

2. A computer program product as claimed in claim 1, wherein one of said at least one secondary set of one or more external program calls precedes said primary set of one or more external program calls within said stream of external program calls.

3. A computer program product as claimed in claim 1, wherein said external program calls are application program interface calls to an operating system.

4. A computer program product as claimed in claim 1, wherein each of said external program calls has one or more characteristics compared against said set of rules.

5. A computer program product as claimed in claim 4, wherein said one or more characteristics include:

a call name;

a return address;

one or more parameter values; and

one or more returned results.

6. A computer program product as claimed in claim 1, wherein rules within said set of rules specify score values of external program calls having predetermined characteristics and a set of one or more external program calls is identified as corresponding to malicious computer program activity if said set of one or more external program calls has a combined score value exceeding a threshold level.

7. A computer program product as claimed in claim 6, wherein score values within said set of rules associated with said secondary set of one or more external program calls are increased to more strongly associate said secondary set of external program calls with malicious computer program activity.

8. A computer program product as claimed in claim 1, wherein said set of rules include at least one of:
one or more pattern matching rules; and
one or more regular expression rules.

9. A computer program product as claimed in claim 1, wherein said set of rules are responsive to ordering of external program calls.

10. A computer program product as claimed in claim 1, wherein said modifying code dynamically adapts said set of rules in response to detected streams of external program calls performing malicious computer program activity.

11. A computer program product as claimed in claim 1, wherein at least changes within said set of rules are transmitted to one or more remote computer such that said one or more remote computers can use said modified set of rules without having to suffer said malicious computer program activity.

12. A computer program product as claimed in claim 1, wherein changes within said set of rules are transmitted to a rule supplier.

13. A computer program product as claimed in claim 1, wherein said stream of external program calls are logged following emulation of execution of a computer program.

14. A computer program product as claimed in claim 1, wherein said set of rules is modified to include a new rule corresponding to said secondary set of one or more external program calls, said new rule thereafter being used in addition to other rules within said set of rules.

15. A computer program product as claimed in claim 1, comprising starting point identifying code operable to identify a starting point of malicious computer program activity within said stream of external program calls.

16. A computer program product as claimed in claim 15, wherein said starting point corresponds to one of:

starting execution of a computer file; and

a switch of memory address region from which program instruction are executed.

17. A computer program product as claimed in claim 1, wherein said set of rules is subject to a validity check after modification to determine if said set of rules is more effectively detecting malicious computer program activity.

18. A method of detecting malicious computer program activity, said method comprising the steps of:

logging a stream of external program calls;

identifying within said stream of external program calls a primary set of one or more external program calls matching one or more rules indicative of malicious computer program activity from among a set of rules;

identifying within said stream at least one secondary set of one or more external program calls associated with said primary set of one or more external program calls; and

modifying said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity.

19. A method as claimed in claim 18, wherein one of said at least one secondary set of one or more external program calls precedes said primary set of one or more external program calls within said stream of external program calls.

20. A method as claimed in claim 18, wherein said external program calls are application program interface calls to an operating system.

21. A method as claimed in claim 18, wherein each of said external program calls has one or more characteristics compared against said set of rules.

22. A method as claimed in claim 21, wherein said one or more characteristics include:

a call name;

a return address;

one or more parameter values; and

one or more returned results.

23. A method as claimed in claim 18, wherein rules within said set of rules specify score values of external program calls having predetermined characteristics and a set of one or more external program calls is identified as corresponding to malicious computer program activity if said set of one or more external program calls has a combined score value exceeding a threshold level.

24. A method as claimed in claim 23, wherein score values within said set of rules associated with said secondary set of one or more external program calls are increased to more strongly associate said secondary set of external program calls with malicious computer program activity.

25. A method as calimed in claim 18, wherein said set of rules include at least one of:

one or more pattern matching rules; and

one or more regular expression rules.

26. A method as claimed in claim 18, wherein said set of rules are responsive to ordering of external program calls.

27. A method as claimed in claim 18, wherein said step of modifying said set of rules dynamically adapts said set of rules in response to detected streams of external program calls performing malicious computer program activity.

28. A method as claimed in claim 18, wherein at least changes within said set of rules are transmitted to one or more remote computer such that said one or more remote computers can use said modified set of rules without having to suffer said malicious computer program activity.

29. A method as claimed in claim 18, wherein changes within said set of rules are transmitted to a rule supplier.

30. A method as claimed in claim 18, wherein said stream of external program calls are logged following emulation of execution of a computer program.

31. A method as claimed in claim 18, wherein said set of rules is modified to include a new rule corresponding to said secondary set of one or more external program calls, said new rule thereafter being used in addition to other rules within said set of rules.

32. A method as claimed in claim 18, comprising identifying a starting point of malicious computer program activity within said stream of external program calls.

33. A method as claimed in claim 32, wherein said starting point corresponds to one of:

starting execution of a computer file; and

a switch of memory address region from which program instruction are executed.

34. A method as claimed in claim 18, wherein said set of rules is subject to a validity check after modification to determine if said set of rules is more effectively detecting malicious computer program activity.

35. A data processing apparatus operable to detect malicious computer program activity, said apparatus comprising:

logging logic operable to log a stream of external program calls;

primary set identifying logic operable to identify, within said stream of external program calls, a primary set of one or more external program calls matching one or more rules indicative of malicious computer program activity from among a set of rules;

secondary set identifying logic operable to identify, within said stream, at least one secondary set of one or more external program calls associated with said primary set of one or more external program calls; and

modifying logic operable to modify said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity.

36. An apparatus as claimed in claim 35, wherein one of said at least one secondary set of one or more external program calls precedes said primary set of one or more external program calls within said stream of external program calls.

37. An apparatus as claimed in claim 35, wherein said external program calls are application program interface calls to an operating system.

38. An apparatus as claimed in claim 35, wherein each of said external program calls has one or more characteristics compared against said set of rules.

39. An apparatus as claimed in claim 38, wherein said one or more characteristics include:

a call name;

a return address;

one or more parameter values; and

one or more returned results.

40. An apparatus as claimed in claim 35, wherein rules within said set of rules specify score values of external program calls having predetermined characteristics and a set of one or more external program calls is identified as corresponding to malicious computer program activity if said set of one or more external program calls has a combined score value exceeding a threshold level.

41. An apparatus as claimed in claim 40, wherein score values within said set of rules associated with said secondary set of one or more external program calls are increased to more strongly associate said secondary set of external program calls with malicious computer program activity.

42. An apparatus as claimed in claim 35, wherein said set of rules include at least one of:

one or more pattern matching rules; and

one or more regular expression rules.

43. An apparatus as claimed in claim 35, wherein said set of rules are responsive to ordering of external program calls.

44. An apparatus as claimed in claim 35 wherein said modifying logic dynamically adapts said set of rules in response to detected streams of external program calls performing malicious computer program activity.

45. An apparatus as claimed in claim 35, wherein at least changes within said set of rules are transmitted to one or more remote computer such that said one or more remote computers can use said modified set of rules without having to suffer said malicious computer program activity.

46. An apparatus as claimed in claim 35, wherein changes within said set of rules are transmitted to a rule supplier.

47. An apparatus as claimed in claim 35, wherein said stream of external program calls are logged following emulation of execution of a computer program.

48. An apparatus as claimed in claim 35, wherein said set of rules is modified to include a new rule corresponding to said secondary set of one or more external program calls, said new rule thereafter being used in addition to other rules within said set of rules.

49. An apparatus as claimed in claim 35, comprising starting point identifying logic operable to identify a starting point of malicious computer program activity within said stream of external program calls.

50. An apparatus as claimed in claim 49, wherein said starting point corresponds to one of:

starting execution of a computer file; and

a switch of memory address region from which program instruction are executed.

51. An apparatus as claimed in claim 35, wherein said set of rules is subject to a validity check after modification to determine if said set of rules is more effectively detecting malicious computer program activity.